CMS (MDCN) EXTRANET DNS REFERENCE FOR CMS BUSINESS PARTNERS (MMA HELP DESK)

CMS

CENTERS for MEDICARE & MEDICAID SERVICES

LOCKHEED MARTIN

We never forget who we're working for™

SUBMITTED BY: LOCKHEED MARTIN
JUNE 30, 2005

This proposal or quotation includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed – in whole or in part – for any purpose other than to evaluate this proposal or quotation. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction.

The data in the pages of this proposal contain trade secrets and commercial or financial information that are either specifically exempted from disclosure by statute or privileged or confidential within the meaning of the exemptions set forth in Section 552(b)(3) and (4), respectively, of the Freedom of Information Act, 5 U.S.C. 552, the disclosure of which could invoke the criminal sanctions of 18 U.S.C. 1905.

TABLE OF CONTENTS

FIGURES

1.0 INTRODUCTION

This document is intended to guide onsite administrators at the Business Partner (BP) in configuring their environment to leverage the CMS (MDCN) Extranet DNS servers accessible via AT&T/MDCN Frame Relay Network. These name servers are dedicated to providing name resolution for CMS Extranet hosted applications located at CMS Central Office (CO). A number of assumptions are made regarding MDCN connectivity requirements and thus impact the guided reference contained herein. Since it's nearly impossible to know the infrastructure for each BP's site, the references made are intended to provide insight and assist BPs but do not necessarily represent the actual configurations required to ensure 100% success without additional modifications as needed.

1.1 Assumptions and Constraints

The following assumptions will be made:

- BPs currently have connectivity to CMS CO infrastructure through the AT&T/MDCN network to the CMS Extranet zone.
- ACLs and FW entries on CMS infrastructure allow UDP:53 traffic from BPs to the Extranet (MDCN) DNS'.
- BPs connected to the MDCN Network can not simultaneously have connectivity to the internet.

The following are constraints:

- If using proxy-type gateway, the gateway must be configured with DNS IPs of an internal DNS server which is "delegatable", implying the DNS server is able to support the delegation of name spaces or conditional forwarding of name spaces (i.e., cmsnet.)
- If BP client workstations are configured with DNS IPs of internal DNS' for access to local LAN resources, the internal DNS' they're using must also be able to support delegation or conditional forwarding of name spaces.

2.0 CMS EXTRANET (MDCN) DNS SERVER OVERVIEW

The MDCN DNS servers will consist of three DNS servers geographically dispersed in secure environments and will be solely dedicated to providing name resolution for CMS Extranet hosted applications. Two of the production MDCN DNS servers (CONDN11 and CONDN12), located at CMS CO, will be hardware load balanced to ensure availability while the third MDCN DNS, located in Kansas City RO, is intended to provide redundancy in the event of a CO outage. MDCN name resolution will resolve a FQDN to the IP of presentation server(s) for the respective applications. Since both MDCN DNS servers (CONDN11 and CONDN12) will be hardware load balanced, BPs will be able to configure their environment using a single virtual IP (VIP) address which transparently maps to each server's IP. Load balancing and failover will be transparent to BPs in this configuration for nodes explicitly configured to resolve from the MDCN DNS'. In situations where a BP's internal DNS is configured for delegation, a single (NS) record will be configured to delegate name queries to the VIP of the CO MDCN DNS' 50% of the time and a second NS record will map to the KC server's IP the remaining 50%. In situations where it's necessary to keep 66% of the MDCN DNS queries local to the CO DNS', traffic may be shaped by simply creating two (NS) name server records mapping to the IPs of each CO MDCN DNS (CONDN11 and CONDN12) and a third NS record mapping to the KC DNS IP. Please refer to specific configuration scenarios below for more details and explanation.

The MDCN name space Top Level Domain (TLD) will be <cmsnet>. Host (A) records will populate the <cmsnet> zone on the Extranet DNS servers. Host records will map a common application "host" name to a single or multiple presentation server(s) IP address(s) in the CMS Extranet zone. In some cases, multiple (A) to IP mapping may exist providing a simplistic method of DNS round-robin load balancing when multiple presentation servers host the same application and transactions are low. Applications with multiple presentation servers experiencing a high number of transactions may be balanced using a hardware device in which only a single (A) record to IP mapping is hosted on the DNS for the respective application.

A key assumption: BPs who currently have connectivity via AT&T/MDCN must not simultaneously have connectivity to the internet. That being said, a number of BP configuration scenarios can be conceptualized with the intent to assist BP Site Administrators in configuring their nodes so they can successfully leverage the MDCN DNS' for name resolution (see below).

Note: The information provided below is based on specific knowledge regarding the CMS past/present infrastructure and general knowledge with technology. It is merely intended to provide some insight while configuring the BP site to resolve <cmsnet> name queries and provide some level of failover in the event the CO MDCN DNS servers with out impacting the existing BP infrastructure.

The following list of configuration scenarios will be discussed in detail and are provided as reference for BP site administrators:

- LAN Workstations/Servers for Direct Access
  - ➢ Nodes dedicated for access to CMS (MDCN) Extranet
  - ➢ Only able to use MDCN DNS servers

- ➢ Workstation/Server Sourced Traffic
- Web Proxy Clients Connect via Proxy Server Dedicated for Intranet Site Connectivity (See section 1.1 MDCN connectivity "mandate/regulation" reference)
  - ➢ Proxy Name Resolution via Internal DNS, implying delegation or conditional forwarding required (Root Hints and/or Forwarders Unaffected)
  - ➢ Proxy Name Resolution via MDCN DNS; Internal DNS NOT used, implying proxy explicitly configured with IP of MDCN DNS servers only (Proxy Direct Access)
  - ➢ Proxy Sourced Traffic
- Web Proxy Clients for Direct Access
  - ➢ Name resolution via MDCN DNS
  - ➢ Web Proxy Clients configured with (IE) Web Proxy exceptions (i.e., cmsnet> name space or IP ranges for destination nodes)
  - ➢ Web Proxy Client Sourced Traffic

2.1 LAN Workstations/Servers for Direct Access – "Client Sourced Traffic"

This configuration represents situations where nodes are dedicated for CMS (MDCN) Extranet connectivity and traffic is sourced from workstation/servers with direct connectivity to the MDCN DNS and CMS Extranet Presentation Servers. Users of these nodes may open a browser and type the Fully Qualified Domain Name (FQDN) for access to an Extranet hosted application (Example: "<app_name.cmsnet>). Configuration requirements are as follows:

2.1.1 Assumptions

- Dedicated nodes don't require internal name resolution for BP LAN resources, hence the reference "dedicated".
- Nodes already have end to end IP connectivity via AT&T/MDCN for application (most cases TCP:80/443) and DNS related traffic (UDP:53).

2.1.2 Configuration Summary

- BP workstations/servers DNS IP settings
  - ➢ Primary = VIP of CO (MDCN) DNS which transparently maps to both CO MDCN DNS servers, CONDN11 and CONDN12
  - ➢ Secondary = IP of KC (MDCN) DNS

- DNS Suffix Search List: Although not required, BPs may add <cmsnet> in the DNS suffix search list for client/server DNS IP settings. Resolver (either client/server in this case) appends the parent name of the domain it's a member of to the original FQDN and unqualified queries by default, **if a suffix search list is not configured.** If a suffix search list is configured, then the client/server defaults to sequentially appending and querying the suffix search list to the original unqualified and FQDN queries. In either case (suffix search configured or not configured), original **FQDN** queries would be attempted and resolved by the authoritative MDCN DNS Servers.
- Client/Server web browsers would NOT be configured for a proxy server, implying traffic is sourced from the dedicated client workstation or server.

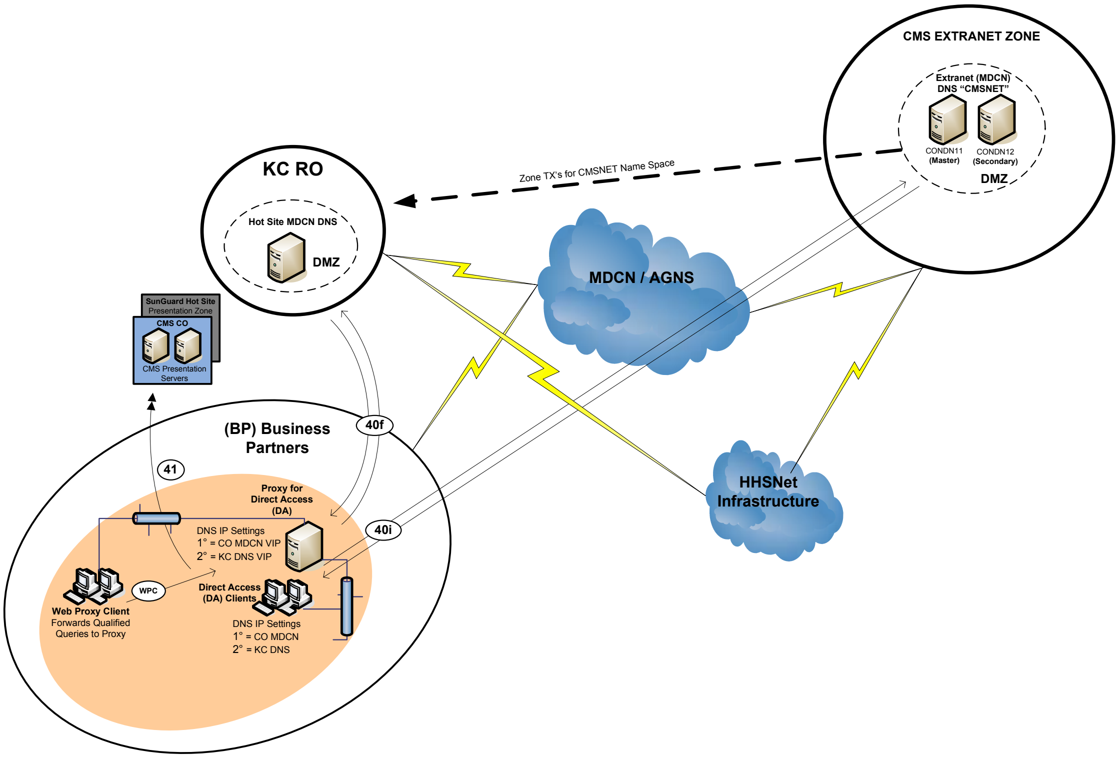
2.1.3 Scenario - Signal Path of Traffic: User queries FQDN <app_name.cmsnet> from (IE) Browser

User opens browser which is auto-configured to detect connection settings. Auto-configuration script is not being used and browser is not configured to use a proxy server; therefore, browser web proxy exceptions are not populated. User types <app_name.cmsnet> in browser. Node contacts the first (primary) DNS IP configured which happens to be a single VIP transparently mapping to the two MDCN DNS servers located at CMS CO (CONDN11 and CONDN12). The following two outcomes are possible from this point forward:

1. CO MDCNs are online and able to respond authoritatively resolving the FQDN to an IP.
2. Both CO MDCN DNS servers are unavailable due to system failures or data communication outages. In this case, the client/server (called the "Resolver") would default to querying the secondary DNS IP configured and restart the original query. The secondary DNS IP configured is the Kansas City Regional Office (RO) DNS IP. Connectivity to this redundant DNS server located in KC is also accessible via the AT&T/MDCN network, has a complete copy of the <cmsnet> zone data, and will successfully resolve the query to the IP of the target host (Presentation Server) located in the CMS CO Extranet.

Client/Server receives the IP, caches the queried response, and contacts the destination presentation server via the AT&T/MDCN network.

Figure 1— Logical DNS Topology - Workstations/Servers for Direct Access



2.2 Web Proxy Clients Connect via Proxy Server Dedicated for Intranet Site Connectivity – "Proxy Sourced Traffic"

As stated in section 1.1, one key assumption states BPs with connectivity to MDCN/AT&T network can not simultaneously have connectivity to the internet. Under that assumption, we can proceed to discuss a number of possible proxy-related configurations describing name resolution and routing of traffic destined for BP intranet sites and MDCN connectivity. Traffic can be sourced from the client or from the proxy node – it really depends on whether the BP infrastructure (ACLs and FWs) allow client-sourced traffic to the CMS Extranet hosted applications.

A proxy in this scenario would not be communicating via the internet for any kind of traffic if the node also has connectivity to MDCN and is used by LAN clients to connect to CMS (MDCN) Extranet hosted applications. This is an important factor because it tells us the proxy's DNS IP settings would NOT be pointing to any external name servers. Instead, a proxy in this scenario may be:

- Pointing to the BPs internal DNS or another private stealth mode DNS server(s) via WAN links from which it is currently configured to resolve name queries, or,
- May be explicitly configured for only the CMS MDCN DNS servers.

The front end of many applications are web-based, thus require a browser like Internet Explorer (IE) to access the application front end. This is the case for many of the CMS Extranet hosted applications in the presentation zone.

Generally speaking, BP workstations (Web Proxy Client) IE proxy settings would be configured with the IP or FQDN of the proxy node(s) in order to route traffic through the dedicated gateway. A number of possible configurations follow, based on the concept of a proxy dedicated for intranet site-based connectivity and LAN clients configured to use the proxy via the MDCN network.

2.2.1 General Requirements

- BP infrastructure (Routers and FWs) allow proxy and client sourced UDP:53 and in/out-bound application related traffic.

2.2.2 Assumptions

- Proxy server is dedicated solely for intranet site connectivity, implying is not proxying on behalf of client internet requests (see section 1.1).
- If proxy is configured to use an internal DNS server, the internal DNS supports the delegation or conditional forwarding.
- BP proxy already has end to end IP connectivity via AT&T/MDCN for application (most cases TCP:80/443) and DNS related traffic (UDP:53).
- Web Proxy Client's (IE) browsers are configured to use the proxy and client does NOT have Web Proxy exceptions for CMS Extranet hosted applications (i.e., web proxy exceptions like <*.cmsnet> or IP ranges with wild cards for subnet ranges like <158.73*> for traffic destined for the CMS Extranet Presentation servers.
- The expectation is that DHCP or statically configured clients have a primary and secondary internal DNS IP setting used to resolve BP LAN resources on their local infrastructure.

2.2.3 Configuration Summary

- Web Proxy Client
  - ➢ Client DNS IP Settings: Client primary and secondary DNS IP settings can be configured for the BP internal DNS servers with out impacting this scenario
  - ➢ Client (IE) browser must be configured to use the proxy server
  - ➢ Client (IE) browser must NOT be configured with Web Proxy exception entries for <*.cmsnet> or IP ranges for traffic destined for the CMS Extranet as this will cause the Web Proxy Client to by-pass the Web Proxy service on the Proxy server and attempt "Direct Access" which is not desirable in this scenario.

- PROXY
  - Proxy Name Resolution via BP Internal DNS
    - Proxy must not be configured for an external DNS which is not a problem, per mandate stated in section 1.1 (Note: Internal DNS' delegating the <cmsnet> name space out to the MDCN DNS').
    - Name resolution to internal DNS servers providing access to BP LAN or private WAN resources should not be impacted since the internal DNS will simply delegate out the <cmsnet> name space to the MDCN DNS'. This allows an existing proxy server to continue responding/servicing Web Proxy Client requests for BP intranet related resources while simultaneously serving additional Web Proxy Client requests for CMS Extranet bound traffic on behalf of BP LAN clients.
    - BP internal DNS' must delegate or conditionally forward the <cmsnet> name space out to the MDCN DNS servers as such:

      Delegation (50:50) CO:KC MDCN DNS Traffic Balance

      - Create a new domain/zone on the primary internal DNS server called "cmsnet"
      - Remove any (NS) records created during zone creation
      - Add a single (NS) Name Server record mapping to the VIP of the CO MDCN DNS servers (CONDN11 and CONDN12)
      - Add a second (NS) record mapping to the KC MDCN DNS IP

      Conditional Forwarding – 100% MDCN DNS Traffic to CO, or 100% MDCN DNS Traffic to KC DNS with CO Outage

      - On the internal DNS servers, locate applet/parameter providing the means to specify a name space filter – this "filter" is nothing more than a qualifier for the internal DNS, such that when it receives a query, the internal DNS parses conditional forwarding query list for a match prior to attempting to answer the query itself. If a match is found, the query is explicitly forwarded to a destination DNS server of choice you configure.
        - Conditional Forwarding Filter = "cmsnet"
        - Destination DNS for this filter
          - Primary = VIP for the CO MDCN DNS servers
          - Secondary = IP for KC MDCN DNS
        - Proxy Name Resolution via MDCN DNS Only
          - Proxy must NOT be configured for an external DNS which is not a problem, per mandate stated in section 1.1

- Proxy must NOT be configured for any other DNS IP other than the MDCN DNS server IPs as stated below – this is "DNS by design".
- Proxy DNS IP Settings:
  - Primary = VIP of CO (MDCN) DNS which transparently maps to both CO MDCN DNS servers, CONDN11 and CONDN12
  - Secondary = IP of KC (MDCN) DNS

2.2.4 Scenario - Signal Path of Traffic: Web Proxy Client queries FQDN <app_name.cmsnet> from (IE) Browser

User opens browser which is auto-configured to detect connection settings. Browser settings are either auto-configured via a configuration script or manually configured to use a proxy server. User types <app_name.cmsnet> in browser. No exception entries found matching the query for the TLD queried (cmsnet) so the Web Proxy Client does not by-pass the Web Proxy Service on the Proxy server. HTTP(S) "GET" request handed to the proxy server for processing on behalf of the client. The following outcomes are possible depending on the proxy server DNS IP configurations:

1. Proxy Name Resolution via BP Internal DNS

   a. Internal DNS with Delegation (50:50 Balance)

      Proxy server (now the "Resolver") queries the first (primary) DNS IP configured which is the BP internal DNS. The BP internal DNS configured to delegate the <cmsnet> name space then round-robins the 2 (NS) records present in the <cmsnet> zone and provides one NS record back to the proxy server as a referral. In this case, the referral provided was to the CO MDCN DNS'. The proxy server attempts to contact the CO MDCN DNS VIP which transparently maps to two DNS servers (CONDN11 and COND12). Should these two DNS servers be offline or not accessible, the proxy server would query the internal DNS again which would round robin a referral (NS) record pointing to the KC MDCN DNS. The proxy proceeds to contact the KC DNS which resolves the FQDN to an IP and returns an authoritative response.

   The proxy server caches this response, contacts the destination node, and processes the "GET" request on behalf of the Web Proxy Client (see Figure 2).

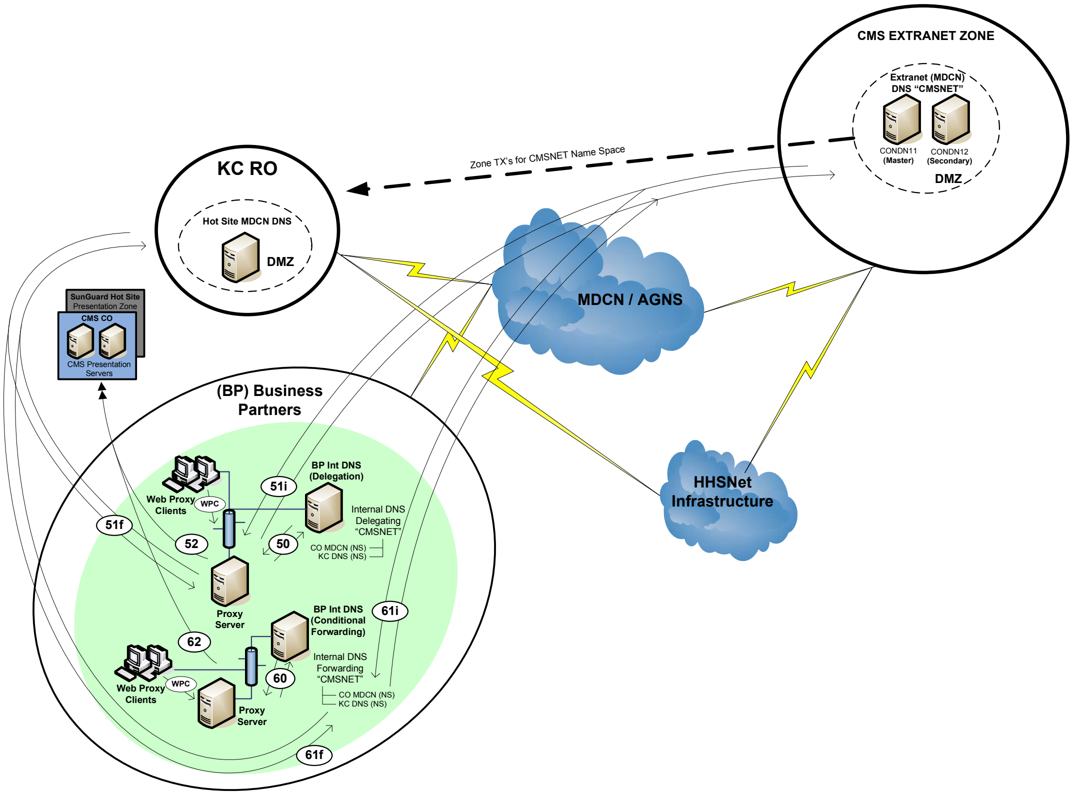
   b. Internal DNS with Conditional Forwarding (100% MDCN DNS Queries Destined for CO MDCN DNS' – Unless CO Outage).

      Proxy server queries the first (primary) DNS IP configured which is the BP internal DNS. Recall, the BP internal DNS is configured to conditionally forward <cmsnet> queries in this scenario. **Please note: It's the BP internal DNS which has now become the "Resolver" and attempts to resolve the query by contacting the forwarder listed, which is the**

MDCN DNS, on behalf of the proxy server. The BP internal DNS configured to "conditionally forward" <cmsnet> name queries first to the CO MDCN DNS(s) and secondarily to the KC MDCN DNS, will attempt to query the CO MDCN DNS VIP which transparently maps to two DNS servers (CONDN11 and COND12). Should these two DNS servers be offline or not accessible, the BP internal DNS server would default to the Secondary Forwarder listed and query the KC MDCN DNS. The BP internal DNS proceeds to contact the KC DNS which resolves the FQDN to an IP and returns an authoritative response to the BP internal DNS which hands the IP to the proxy.

The BP internal DNS (Resolver #2) and proxy (Resolver #1) both cache this response, the proxy contacts the destination node, and processes the "GET" request on behalf of the Web Proxy Client (see Figure 2).

Figure 2— Logical DNS Topology - Proxy Server Sourced Traffic



2. Proxy Name Resolution via MDCN DNS Only

   Proxy server becomes the "Resolver" and queries the first (primary) DNS IP configured which happens to be a single VIP transparently mapping to the two MDCN DNS servers located at CMS CO (CONDN11 and CONDN12). The following two outcomes are possible from this point forward:

   a. CO MDCNs are online and able to respond authoritatively resolving the FQDN to an IP.

   b. CO MDCN DNS servers are unavailable due to system failures or data communication outages. In this case, the proxy ("Resolver") would default to querying the secondary DNS IP configured and restart the original query. The secondary DNS IP configured is the Kansas City Regional Office (RO) DNS IP. Connectivity to this redundant DNS server located in KC is also accessible via the AT&T/MDCN network, has a complete copy of the <cmsnet> zone data, and will successfully resolve the query to the IP of the target host (Presentation Server) located in the CMS CO Extranet.

   The proxy server caches this response, contacts the destination node, and processes the "GET" request on behalf of the Web Proxy Client (see Figure 1).

Special Note: If Web Proxy Clients attempt to query the unqualified name of a MDCN destination host for access to a CMS Extranet Hosted Application (i.e., instead of querying the FQDN "app_name.cmsnet" the client queries "app_name" the following undesired outcomes would result:

a. The Web Proxy Client by default would not hand the request off to the proxy server for resolution/processing – this is DNS by-design…… fully qualifying the query with a dot "." forces a Web Proxy Client to hand the request to the configured proxy node. Unqualified queries (such as <app_name>) from a Web Proxy Client may be successful if the client's DNS suffix search list is configured with an entry for "cmsnet" – testing is necessary prior to implementation to be sure client's browser attempts to append the suffix search list entries for unqualified queries in the browser window.

b. The client would certainly fail to resolve unqualified name queries without, and potentially still fail, with additional modifications/configurations to DNS suffix search lists.

2.3 Web Proxy Clients for Direct Access – "Web Proxy Client Sourced Traffic"

In this scenario, traffic is sourced from the Web Proxy Client. LAN clients are by passing the proxy server for access to CMS Extranet hosted applications via the MDCN network. Here, the LAN client's own DNS IP settings will be used to resolve the FQDN to and IP and will use IP routing to reach the destination via the MDCN network. In order for a Web Proxy Client to by pass a proxy server, Web Proxy expectations entries must be configured in the client's browser.

2.3.1 Assumptions

- DHCP configured or statically configured Web Proxy Clients have primary and secondary DNS IPs configured.
- BP LAN clients 1) use their (IE) browsers to access CMS Extranet hosted applications via a (web front end) presentation server 2) if client's browsers are configured with the host name or IP of a proxy device, their browser has web proxy exceptions entries for CMS Extranet hosted resources (i.e., IP ranges or wild cards for name spaces such as <*.cmsnet>).
- DNS suffix search lists on client desktops should not need to be modified since queries are first appended with the suffix search list in order until a successful response is received. If the query is not resolved after parsing the suffix search list, the query is attempted without appending anything and will successfully resolve the originally queried FQDN <app_name.cmsnet>.

2.3.2 Configuration Summary

- Web Proxy Client
  - ➢ Client (IE) browser must be configured to use the proxy server
  - ➢ Client (IE) browser MUST be configured with Web Proxy exception entries for <*.cmsnet> or IP ranges for traffic destined for the CMS Extranet as this will cause the Web Proxy Client to by-pass the Web Proxy service on the Proxy server and attempt "Direct Access"
  - ➢ Web Proxy Client Name Resolution via BP Internal DNS
    - ▪ Name resolution to internal DNS servers providing access to BP LAN or private WAN resources should not be impacted since the internal DNS will simply delegate out the <cmsnet> name space to the MDCN DNS'. This allows the Web Proxy Clients to continue resolving BP internal name spaces for access to resources.
    - ▪ BP internal DNS' must delegate or conditionally forward the <cmsnet> name space out to the MDCN DNS servers as such:

      Delegation (50:50) CO:KC MDCN DNS Traffic Balance

      - Create a new domain/zone on the primary internal DNS server called "cmsnet"
      - Remove any (NS) records created during zone creation
      - Add a single (NS) Name Server record mapping to the VIP of the CO MDCN DNS servers (CONDN11 and CONDN12)
        - ▪ Add a second (NS) record mapping to the KC MDCN DNS IP

      Conditional Forwarding – 100% MDCN DNS Traffic to CO, or 100% MDCN DNS Traffic to KC DNS with CO Outage

- On the internal DNS servers, locate applet/parameter providing the means to specify a name space filter – this "filter" is nothing more than a qualifier for the internal DNS, such that when it receives a query, the internal DNS parses conditional forwarding query list for a match prior to attempting to answer the query itself. If a match is found, the query is explicitly forwarded to a destination DNS server of choice you configure.
    - Conditional Forwarding Filter = "cmsnet"
    - Destination DNS for this filter
        - Primary = VIP for the CO MDCN DNS servers
        - Secondary = IP for KC MDCN DNS
- Web Proxy Client Name Resolution via MDCN DNS Only
    - Web Proxy Client must NOT be configured for any other DNS IP other than the MDCN DNS server IPs as stated below – this is "DNS by design".
    - Web Proxy Client DNS IP Settings:
        - Primary = VIP of CO (MDCN) DNS which transparently maps to both CO MDCN DNS servers, CONDN11 and CONDN12
        - Secondary = IP of KC (MDCN) DNS

2.3.3 *Scenario - Signal Path of Traffic: Web Proxy Client queries FQDN <app_name.cmsnet> from (IE) Browser*

User opens browser which is auto-configured to detect connection settings. Browser settings are either auto-configured via a configuration script or manually configured to use a proxy server. User types <app_name.cmsnet> in browser. Exception entries found matching the query for the TLD queried (cmsnet) so the Web Proxy Client by-passes the Web Proxy Service on the Proxy server. The following outcomes are possible depending on the Web Proxy Client DNS IP configurations:

1. Web Proxy Client Name Resolution via BP Internal DNS
    a. Internal DNS with Delegation (50:50 Balance)

    Web Proxy Client ("Resolver") queries the first (primary) DNS IP configured which is the BP internal DNS. The BP internal DNS configured to delegate the <cmsnet> name space then round-robins the 2 (NS) records present in the <cmsnet> zone and provides one NS record back to the Web Proxy Client as a referral. In this case, the referral provided was to the CO MDCN DNS'. The Web Proxy Client attempts to contact the CO MDCN DNS VIP which transparently maps to two DNS servers (CONDN11 and COND12). Should these two DNS servers be offline or not accessible, the Web Proxy

Client would query the internal DNS again which would round robin a referral (NS) record pointing to the KC MDCN DNS. The Web Proxy Client would proceed to contact the KC DNS which resolves the FQDN to an IP and returns an authoritative response.

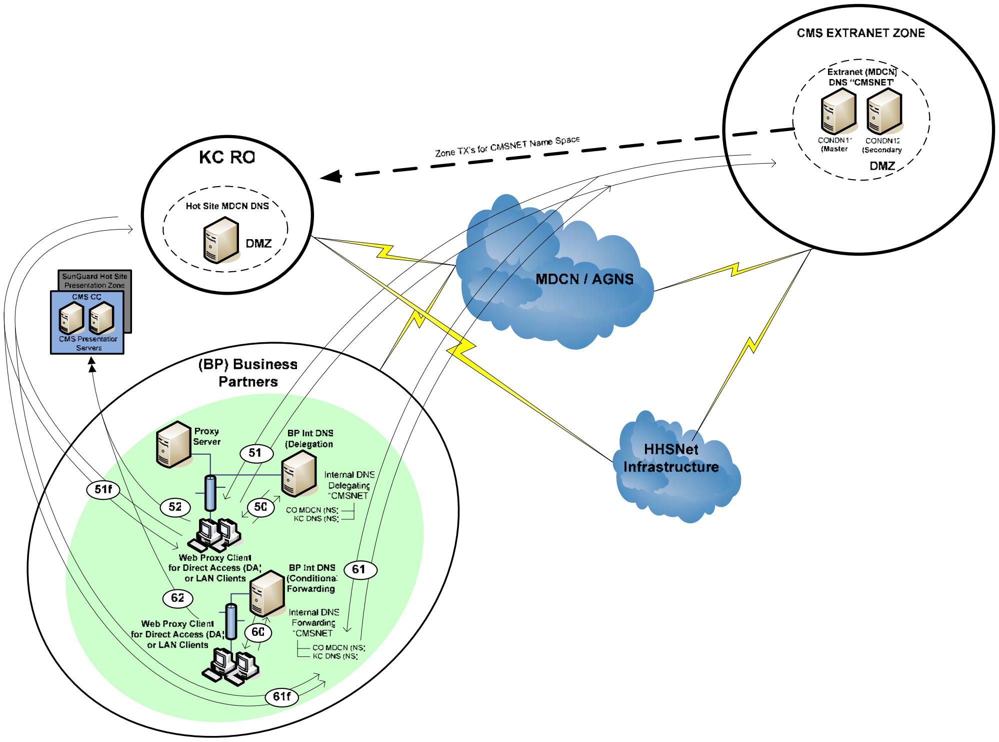
The Web Proxy Client caches this response, contacts the destination node, and processes the "GET" request itself (See Figure 3).

b. Internal DNS with Conditional Forwarding (100% MDCN DNS Queries Destined for CO MDCN DNS' – Unless CO Outage)

Web Proxy Client queries the first (primary) DNS IP configured which is the BP internal DNS. Recall, the BP internal DNS is configured to conditionally forward <cmsnet> queries in this scenario. **Please note: It's the BP internal DNS which has now become the "Resolver" and attempts to resolve the query by contacting the forwarder listed, which is the MDCN DNS, on behalf of the Web Proxy Client.** The BP internal DNS is configured to "conditionally forward" <cmsnet> name queries first to the CO MDCN DNS(s) and secondarily to the KC MDCN DNS. The BP internal DNS will attempt to query the CO MDCN DNS VIP which transparently maps to the two CO MDCN DNS servers (CONDN11 and COND12). Should these two DNS servers be offline or not accessible, the BP internal DNS server would default to the Secondary Forwarder listed and query the KC MDCN DNS. The BP internal DNS proceeds to contact the KC DNS which resolves the FQDN to an IP and returns an authoritative response to the BP internal DNS which returns a non-authoritative response to the Web Proxy Client.

The BP internal DNS (Resolver #2) and Web Proxy Client (Resolver #1) both cache this response, and the Web Proxy Client processes it's own "GET" request and contacts the destination node (See Figure 3).

Figure 3— Logical DNS Topology - Web Proxy Client Sourced Traffic


CMS EXTRANET ZONE
Extranet (MDCN) DNS "CMSNET"
CONDN11 (Master
CONDN12 (Secondary
DMZ
Zone TX's for CMSNET Name Space
KC RO
Hot Site MDCN DNS
DMZ
MDCN / AGNS
HHSNet Infrastructure
SunGuard Hot Site Presentation Zone
CMS CC
CMS Presentation Servers
(BP) Business Partners
Proxy Server
BP Int DNS (Delegation
51
51f
52
50
Internal DNS Delegating "CMSNET
CO MDCN (NS)
KC DNS (NS)
Web Proxy Client for Direct Access (DA) or LAN Clients
BP Int DNS (Conditional Forwarding
61
62
60
Internal DNS Forwarding "CMSNET
CO MDCN (NS)
KC DNS (NS)
Web Proxy Client for Direct Access (DA) or LAN Clients
61f

2. Web Proxy Client Name Resolution via MDCN DNS Only (a.k.a, Direct Access Nodes)

   Web Proxy Client is the only "Resolver" in this scenario and queries the first (primary) DNS IP configured which happens to be a single VIP transparently mapping to the two MDCN DNS servers located at CMS CO (CONDN11 and CONDN12). The following two outcomes are possible from this point forward:

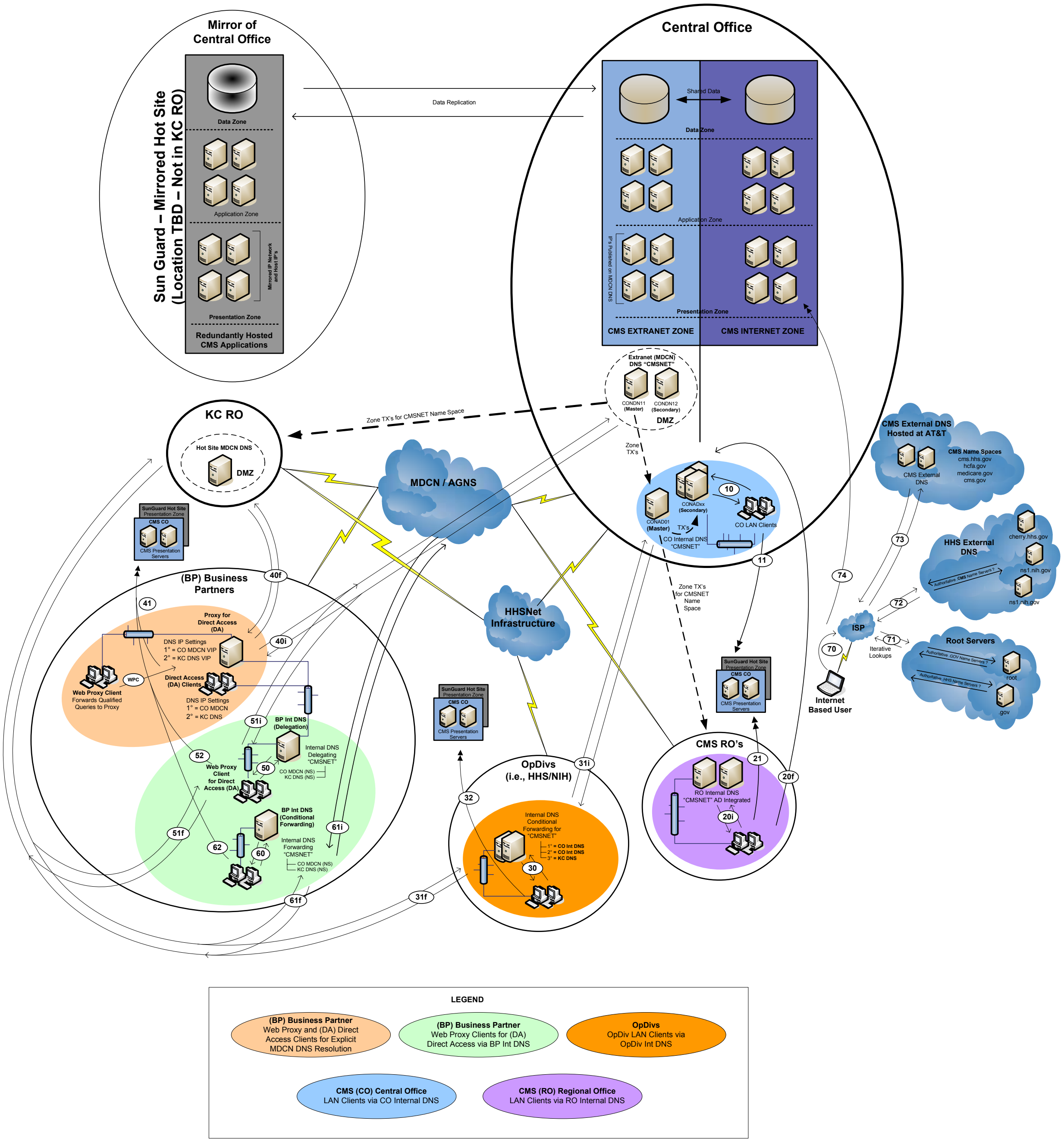
   a. CO MDCNs are online and able to respond authoritatively resolving the FQDN to an IP.

b. CO MDCN DNS servers are unavailable due to system failures or data communication outages. In this case, the Web Proxy Client ("Resolver") would default to querying the secondary DNS IP configured and restart the original query. The secondary DNS IP configured is the Kansas City Regional Office (RO) DNS IP. Connectivity to this redundant DNS server located in KC is also accessible via the AT&T/MDCN network, has a complete copy of the <cmsnet> zone data, and will successfully resolve the query to the IP of the target host (Presentation Server) located in the CMS CO Extranet.

The Web Proxy Client caches this response, contacts the destination node, and processes the "GET" request itself (similar to Direct Access Nodes - See Figure 1).

APPENDIX A — CMS COMPREHENSIVE MDCN DNS TOPOLOGY

**CMS Logical MDCN DNS Topology for
CMS Extranet / Internet Zones**


Mirror of Central Office
Sun Guard – Mirrored Hot Site (Location TBD – Not in KC RO)
Data Zone
Application Zone
Mirrored IP Network and Host IP's
Presentation Zone
Redundantly Hosted CMS Applications
Data Replication
Central Office
Shared Data
Data Zone
Application Zone
IP's Published on MDCN DNS
Presentation Zone
CMS EXTRANET ZONE
CMS INTERNET ZONE
Extranet (MDCN) DNS "CMSNET"
CONDN11 (Master)
CONDN12 (Secondary)
DMZ
Zone TX's for CMSNET Name Space
Zone TX's
CONAD01 (Master)
CONADxx (Secondary)
TX's
10
CO LAN Clients
CO Internal DNS "CMSNET"
11
KC RO
Hot Site MDCN DNS
DMZ
MDCN / AGNS
HHSNet Infrastructure
SunGuard Hot Site Presentation Zone
CMS CO
CMS Presentation Servers
(BP) Business Partners
40f
41
40i
Proxy for Direct Access (DA)
DNS IP Settings
1° = CO MDCN VIP
2° = KC DNS VIP
WPC
Web Proxy Client
Forwards Qualified Queries to Proxy
Direct Access (DA) Clients
DNS IP Settings
1° = CO MDCN
2° = KC DNS
51i
BP Int DNS (Delegation)
Internal DNS Delegating "CMSNET"
CO MDCN (NS)
KC DNS (NS)
52
Web Proxy Client for Direct Access (DA)
50
BP Int DNS (Conditional Forwarding)
Internal DNS Forwarding "CMSNET"
CO MDCN (NS)
KC DNS (NS)
51f
62
60
61i
61f
31f
OpDivs (i.e., HHS/NIH)
31i
32
Internal DNS Conditional Forwarding for "CMSNET"
1° = CO Int DNS
2° = CO Int DNS
3° = KC DNS
30
Zone TX's for CMSNET Name Space
CMS RO's
21
20f
RO Internal DNS "CMSNET" AD Integrated
20i
CMS External DNS Hosted at AT&T
CMS External DNS
CMS Name Spaces
cms.hhs.gov
hcfa.gov
medicare.gov
cms.gov
73
74
HHS External DNS
cherry.hhs.gov
ns1.nih.gov
ns1.nih.gov
Authoritative .CMS Name Servers ?
72
ISP
71
70
Iterative Lookups
Internet Based User
Root Servers
Authoritative .GOV Name Servers ?
Authoritative .HHS Name Servers ?
root
.gov
LEGEND
(BP) Business Partner Web Proxy and (DA) Direct Access Clients for Explicit MDCN DNS Resolution
(BP) Business Partner Web Proxy Clients for (DA) Direct Access via BP Int DNS
OpDivs OpDiv LAN Clients via OpDiv Int DNS
CMS (CO) Central Office LAN Clients via CO Internal DNS
CMS (RO) Regional Office LAN Clients via RO Internal DNS

APPENDIX B — EXTRANET (MDCN) DNS TOPOLOGY AND FAILOVER SCENARIOS

(CO) Central Office LAN Users

Configuration State
MDCN DNS
SOA (Zone) threshold values high enough to prevent zone data from timing out on configured Secondary Name Servers (Windows DNS servers)
One MDCN DNS Server is configured to replicate CMSNET zone data to a single Windows internal DNS
LAN Clients
DHCP Scope options allocate a min of two DNS IP settings which point clients to the RO internal DNS server and secondary DNS IP points back to CO internal DNS
Clients are configured with DNS suffix search list: cms.local; hcfa.gov
CMS Internal DNS Servers
Windows Internal DNS receiving the zone copy is configured as a Master Name Server to the remaining CO/RO internal Windows DNS servers

Scenario 1: CO-LAN User Queries "<hostname>.cmsnet"

Step	Comments
10	Client contacts first DNS server in it's DNS IP setting; internal DNS responds authoritatively and resolves "<hostname>.cmsnet" to an IP
11	Client connects to CO Extranet hosted application

Scenario 2: CO-LAN User Queries "<hostname>.cmsnet"

Step	Comments
event	Client's primary DNS IP server is unavailable
10	Client contacts first DNS server in it's DNS IP setting but request times out; client contacts second DNS server (Secondary DNS IP Setting) in list; internal DNS responds authoritatively and resolves "<hostname>" to an IP
11	Client connects to CO Extranet hosted application

Scenario 3: CO-LAN User Queries "<hostname>.cmsnet"

Step	Comments
event	CO MDCN DNS Servers are offline/unavailable but SOA threshold values maintained on the MDCN's are high enough to ensure the zone copy for CMSNET on the Windows internal DNS server doesn't time out
10	Client contacts first DNS server in it's DNS IP setting; internal DNS responds authoritatively and resolves "<hostname>" to an IP
11	Client connects to CO Extranet hosted application

Scenario 4: CO-LAN User Queries "<hostname>.cmsnet"

Step	Comments
event	Catastrophic outage at CO
11-Oct	N/A - (No CO LAN Clients)

(RO) Remote Office LAN Users

Configuration State
MDCN DNS
SOA (Zone) threshold values high enough to prevent zone data from timing out on configured Secondary Name Servers (Windows DNS servers)
One MDCN DNS Server is configured to replicate CMSNET zone data to a single Windows internal DNS
LAN Clients
DHCP Scope options allocate a min of two DNS IP settings which point clients to the RO internal DNS server and secondary DNS IP points back to CO internal DNS
Clients are configured with DNS suffix search list: cms.local; hcfa.gov
CMS Internal DNS Servers
Windows Internal DNS receiving the zone copy is configured as a Master Name Server to the remaining CO/RO internal Windows DNS servers

Scenario 1: RO-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
20i "initial"	Client contacts first DNS server in it's DNS IP setting; RO internal DNS responds authoritatively and resolves "<hostname>.cmsnet" to an IP
21	Client connects to CO Extranet hosted application

Scenario 2: RO-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
event	Client's primary DNS IP server is unavailable
20i "initial"	Client contacts first DNS server in it's DNS IP setting located in the RO but request times out.
20f "failover"	Client contacts second DNS server (Secondary DNS IP Setting) in list located at CO; CO internal DNS responds authoritatively and resolves "<hostname>" to an IP
21	Client connects to CO Extranet hosted application

Scenario 3: RO-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
event	CO MDCN DNS Servers are offline/unavailable but SOA threshold values maintained on the MDCN's are high enough to ensure the zone copy for CMSNET on the Windows CO/RO internal DNS server doesn't time out
20i "initial"	Client contacts first DNS server in it's DNS IP setting; internal DNS responds authoritatively and resolves "<hostname>" to an IP
21	Client connects to CO Extranet hosted application

Scenario 4: RO-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
event	Catastrophic outage at CO
20i "initial"	Client contacts first DNS server in it's DNS IP setting; internal DNS responds authoritatively and resolves "<hostname>" to an IP
21	Client connects to Sun Guard Hot-Site for Extranet hosted application

(OpDivs) Operational Divisions

Configuration State
MDCN DNS
SOA (Zone) threshold values high enough to prevent zone data from timing out on configured Secondary Name Servers (Windows DNS servers)
One MDCN DNS Server is configured to replicate CMSNET zone data to a single Windows internal DNS
BP LAN Clients
DHCP Scope options allocate a min of two DNS IP settings which point clients to the OpDiv's internal DNS servers
CMS Internal DNS Servers
Windows Internal DNS receiving the zone copy is configured as a Master Name Server to the remaining CO/RO internal Windows DNS servers
OpDiv's Internal DNS Servers
OpDiv's internal DNS's are configured for "Conditional Forwarding" and will filter for name queries to the <cmsnet> name space and explicitly forward 1) to CO internal DNS, 2) to second CO internal DNS, and 3) to KC MDCN DNS

Scenario 1: OpDiv-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
30	OpDiv Client contacts it's first internal DNS server in it's DNS IP setting; OpDiv internal DNS explicitly forwards the query to the first CO internal DNS
31i	First CO internal DNS forwarder responds authoritatively and resolves the query to an IP
32	Client connects to CO Extranet hosted application

Scenario 2: OpDiv-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
event	OpDiv Client's primary DNS IP server is unavailable
30	OpDiv Client contacts its own internal DNS which is offline. OpDiv Client contacts it's second internal DNS server (Secondary DNS IP Setting) which responds and is explicitly set to forward <cmsnet> name queries to the first CO internal DNS
31i	OpDiv Client's second internal DNS contacts the CO MDCN DNS which responds authoritatively and resolves the query to an IP
32	OpDiv Client connects to CO Extranet hosted application

Scenario 3: OpDiv-LAN User Queries "<hostname>.cmsnet"	
Step	Comments
event	OpDiv Client's primary DNS IP server is unavailable
event	First CO internal DNS forwarder is unavailable
30	OpDiv Client contacts its first internal DNS server in it's DNS IP setting but request times out. OpDiv Client contacts its second internal DNS server (Secondary DNS IP Setting) which responds and is explicitly set to forward <cmsnet> name queries to the first CO internal DNS
31i	OpDiv internal DNS attempts to query first CO internal DNS forwarder but it's offline so request times out
31f	OpDiv internal DNS attempts to query second forwarder pointing to a second CO internal DNS and it responds authoritatively resolving the query to an IP
32	OpDiv Client connects to CO Extranet hosted application

(OpDivs) Operational Divisions

Scenario 4: OpDiv-LAN User Queries "<hostname>.cmsnet"

Step	Comments
event	CO MDCN DNS Servers are offline/unavailable but SOA threshold values maintained on the MDCN's are high enough to ensure the zone copy for CMSNET on the Windows CO/RO internal DNS server doesn't time out
30	OpDiv Client contacts its first internal DNS server in it's DNS IP setting but request times out. OpDiv Client contacts its second internal DNS server (Secondary DNS IP Setting) which responds and is explicitly set to forward <cmsnet> name queries to the first CO internal DNS
31i	OpDiv internal DNS attempts to query first CO internal DNS forwarder and it responds authoritatively resolving the query to an IP
32	OpDiv Client connects to CO Extranet hosted application

Scenario 5: OpDiv-LAN User Queries "<hostname>.cmsnet"

Step	Comments
event	Catastrophic outage at CO
30	OpDiv Client contacts it's first internal DNS server in it's DNS IP setting; OpDiv internal DNS explicitly forwards the query to the first CO internal DNS
31i	OpDiv internal DNS attempts to query CO MDCN DNS but it's offline so request times out
31i	OpDiv internal DNS attempts to query second forwarder pointing to a second CO internal DNS but it's offline so the query times out
31f	OpDiv internal DNS attempts to query third forwarder which points to the KC MDCN DNS forwarder and it responds authoritatively resolving the query to an IP
32	OpDiv Client connects to Sun Guard Hot-Site for Extranet hosted application

BP Web Proxy & (DA) Direct Access Clients

Configuration State
MDCN DNS
SOA (Zone) threshold values high enough to prevent zone data from timing out on configured Secondary Name Servers (Windows DNS servers)
One MDCN DNS Server is configured to replicate CMSNET zone data to a single Windows internal DNS
BP Direct Access Clients/Servers
Direct Access nodes in this context are nodes which communicate directly with the DNS servers. DA nodes will directly query the CO and KC MDCN DNS servers
Direct Access nodes DNS IP's are configured with their Primary DNS IP=VIP of the CO MDCN DNS's in CO and their Secondary DNS IP=IP of the KC MDCN DNS server

Scenario 1: Web Proxy and (DA) Direct Access Clients Query "<hostname>.cmsnet"	
Step	Comments
WPC	Web Proxy Client queries the FQDN which forces the query to be handled by the proxy since no web proxy exceptions exist in the client's (IE) browser
40i	Proxy is explicitly configured to first use the CO MDCN DNS's which authoritatively resolve the query
41	Proxy receives the IP, caches the response, and processes the GET request on behalf of the Web Proxy Client and connects to the CO Extranet Presentation Server(s)

Scenario 2: Web Proxy and (DA) Direct Access Clients Query "<hostname>.cmsnet"	
Step	Comments
event	CO MDCN DNS servers unavailable
WPC	Web Proxy Client queries the FQDN which forces the query to be handled by the proxy since no web proxy exceptions exist in the client's (IE) browser
40i	Proxy is explicitly configured to first use the CO MDCN DNS's which are unavailable so query times out
40f	Proxy defaults to the secondary DNS IP pointing the KC MDCN DNS which authoritatively resolves the query to an IP
41	Proxy receives the IP, caches the response, and processes the GET request on behalf of the Web Proxy Client

Scenario 3: Web Proxy and (DA) Direct Access Clients Query "<hostname>.cmsnet"	
Step	Comments
event	Catastrophic outage at CO
WPC	Web Proxy Client queries the FQDN which forces the query to be handled by the proxy since no web proxy exceptions exist in the client's (IE) browser
40i	Proxy is explicitly configured to first use the CO MDCN DNS's which are unavailable so query times out
40f	Proxy defaults to the secondary DNS IP pointing the KC MDCN DNS which authoritatively resolves the query to an IP
41	Proxy receives the IP, caches the response, and processes the GET request on behalf of the Web Proxy Client and connects to Sun Guard Hot-Site for the Extranet hosted application

BP Nodes via BP Internal DNS

Configuration State
MDCN DNS
SOA (Zone) threshold values high enough to prevent zone data from timing out on configured Secondary Name Servers (Windows DNS servers)
One MDCN DNS Server is configured to replicate CMSNET zone data to a single Windows internal DNS
BP LAN Clients
BP Web Proxy Clients configured for (DA) via use of web proxy exception entries for <*.cmsnet> and internal LAN clients have a minimum of two DNS IP settings configured which point to the BP's internal DNS Servers
BP Internal DNS Servers
BP internal DNS's configured for 1) Delegation or 2) Conditional Forwarding

Scenario 1: BP Web Proxy Client Queries"<hostname>.cmsnet" and BP Internal DNS w/Delegation	
Step	Comments
50	Web Proxy Client's browser has exception entry for the FQDN queried so by-passes the web proxy service on the proxy server and defaults to contacting it's primary DNS IP which is the BP internal DNS. BP internal DNS is configured to delegate the <cmsnet> name space out to two (NS) name servers: one (NS) Name Server record transparently mapping to two CO MDCN DNS servers and one (NS) record mapping to the KC MDCN DNS…..in this example, the CO MDCN (NS) record is returned to the client.
51i	Web Proxy Client queries the CO MDCN DNS server which authoritatively resolves the query to an IP
52	Web Proxy Client caches the query and contacts the presentation server located in CO

Scenario 2: BP Web Proxy Client Queries"<hostname>.cmsnet" and BP Internal DNS w/Delegation	
Step	Comments
event	CO MDCN DNS servers unavailable **OR** CO Outage
50	Web Proxy Client's browser has exception entry for the FQDN queried so by-passes the web proxy service on the proxy server and defaults to contacting it's primary DNS IP which is the BP internal DNS. BP internal DNS is configured to delegate the <cmsnet> name space out to two (NS) name servers: one (NS) Name Server record transparently mapping to two CO MDCN DNS servers and one (NS) record mapping to the KC MDCN DNS…..in this example, the CO MDCN (NS) record is returned to the client.
51i	Web Proxy Client queries the CO MDCN DNS server which are offline so the query times out
50	Web Proxy Client queries the <cmsnet> name space one more time, the (NS) records round-robin resolve, and the client receives a referral pointing to the KC MDCN DNS
51f	Web Proxy Client queries the KC MDCN DNS which authoritatively responds with the IP of the destination node
52	Web Proxy Client caches the query and contacts the presentation server located in CO

BP Nodes via BP Internal DNS

Scenario 3: BP Web Proxy Client Queries"<hostname>.cmsnet" and BP Internal DNS w/Conditional Forwarding	
Step	Comments
60	Web Proxy Client's browser has exception entry for the FQDN queried so by-passes the web proxy service on the proxy server and defaults to contacting it's primary DNS IP which is the BP internal DNS. BP internal DNS is configured to Conditionally Forward the <cmsnet> name space first to the CO MDCN DNS servers and then to the KC MDCN DNS.
61i	BP internal DNS becomes the resolver and forwards the query to the CO MDCN DNS which resolves the query and returns the IP to the Web Proxy Client
62	Web Proxy Client caches the response and contacts the destination node in the CO Extranet Presentation zone

Scenario 4: BP Web Proxy Client Queries"<hostname>.cmsnet" and BP Internal DNS w/Conditional Forwarding	
Step	Comments
event	CO MDCN DNS servers unavailable **OR** CO Outage
60	Web Proxy Client's browser has exception entry for the FQDN queried so by-passes the web proxy service on the proxy server and defaults to contacting it's primary DNS IP which is the BP internal DNS. BP internal DNS is configured to Conditionally Forward the <cmsnet> name space first to the CO MDCN DNS servers and then to the KC MDCN DNS.
61i	BP internal DNS becomes the resolver and forwards the query to the CO MDCN DNS which is offline so the query times out
61f	BP internal DNS defaults to the second forwarder in the conditional forward filter and forwards the query to the KC MDCN DNS which responds, resolves the FQDN to an IP, and is cached by the internal DNS
62	Web Proxy Client caches the response and contacts the destination node in the CO Extranet Presentation zone